Gerar solução de problemas de dados do software Sourcefire em execução na plataforma BlueCoat X-Series

Contents

Introduction

Um arquivo de solução de problemas contém uma coleção de mensagens de registro, dados de configuração e saídas de comando. É usado para determinar o status de um sistema Sourcefire. Se um engenheiro de suporte da Cisco solicitar que você envie um arquivo de solução de problemas da sua plataforma BlueCoat X-Series (também conhecido como sensor Crosslight), siga as instruções neste documento. Este documento também fornece uma lista dos dados adicionais que podem ser necessários para analisar um problema.

Gerar arquivo de solução de problemas

1. Efetue login no dispositivo BlueCoat X-Series como um usuário admin.

2. Encontre o grupo de VAP para o software Sourcefire.

```
show application vap-group
```

A saída a seguir é um exemplo do comando acima. Neste exemplo, o grupo vap é sf53.

```
VAP Group                    : sf53
App ID : SfSensor
Name : SF Sensor
Version : 5.3.0.1
Release : 55
Start on Boot : yes
App Monitor : on
App State (sf530_1) : Up
```

3. Em seguida, precisamos aumentar o privilégio para que possamos usar o shell remoto no próprio grupo VAP:

```
unix su
```

4. Em seguida, abra uma sessão de shell remoto:

```
rsh
```

Por exemplo,

```
rsh sf53_1
```

5. Agora, carregue o aplicativo específico da Sourcefire:

```
source /opt/sf/profile
```

6. Finalmente, gere uma solução de problemas:

```
sf_troubleshoot.pl -t
```

Solução de problemas adicional

1. Cópias de todos os arquivos /var/log/messages* no Módulo do processador de controle (CPM) são necessárias para análise de log e solução de problemas. Um sensor Sourcefire registra todas as mensagens de syslog no arquivo /var/log/messages de um CPM, em vez de no Application Processor Module (APM), onde o software Sourcefire é executado.

> Note: Observe o * com o comando /var/log/messages*. Use * para incluir todo o arquivo de mensagens do CPM.

2. Uma configuração em execução da plataforma BlueCoat X-Series permite compreender como um sensor é instalado e configurado no XOS. O seguinte comando copia uma configuração em execução em um arquivo de texto:

```
copy running-config /tmp/running_config.txt
```

3. As seguintes saídas de comando são importantes para determinar o status do módulo e do chassi:

```
show module status
```

```
show chassis
```

4. Se um erro ou sintoma for óbvio na interface do usuário da Web, uma captura de tela da interface da Web também será útil para identificar um problema.